noyb - Europäisches Zentrum für digitale Rechte
Goldschlagstraße 172/4/3/2
1140 Wien
ÖSTERREICH

Ad-hoc-Paper (V0.2)
SARS-CoV-2-Verfolgung unter der DSGVO

Im Zuge der Corona-Krise erwägen viele Regierungen und Nichtregierungsorganisationen den Einsatz von Systemen zum Tracking der Ausbreitung von SARS-CoV-2-Infektionen, um die Pandemie zu bekämpfen. Dabei bestehen unterschiedliche Vorstellungen, wie diese Systeme aussehen sollen (siehe Beispiele hier). Im Zuge der Überprüfung einiger dieser Ideen hat *noyb* dieses *Ad-hoc*-Paper über die rechtlichen Anforderungen an derartige Virentracking-Systeme erstellt.

Dieses Paper kann einen allgemeinen und oberflächlichen Überblick über die Mindestanforderungen gemäß der DSGVO und mögliche Strategien zu deren Befolgung geben, es bleibt aber naturgemäß abstrakt und müsste im Hinblick auf spezifische Tracking-Projekte angepasst werden. Wir sind der Meinung, dass die Einhaltung grundlegender Datenschutzbestimmungen entscheidend für die Akzeptanz eines jeden Tracking-Systems durch die Öffentlichkeit ist.

Dieses Paper ist keine Richtlinie und enthält keine politische Bewertung der verschiedenen Tracking-Ansätze. Genauso wenig versucht es, zu beurteilen, welche Datenverarbeitungen aus medizinischer oder statistischer Sicht notwendig wären.

Max Schrems
Geschäftsführer, noyb.eu

➔ Wir beabsichtigen, dieses Paper in den nächsten Tagen und Wochen zu aktualisieren. Bitte informieren Sie sich auf noyb.eu über die neueste Version dieses Papers.

1. UMFANG DIESES Papers (TRACKING-ANWENDUNGEN)

Dieses Paper konzentriert sich auf bekannte technische Methoden zur Verfolgung von Infektionen von Personen mit SARS-CoV-2. Diese Ansätze konzentrieren sich auf Interaktionen zwischen Individuen, bei denen diese Interaktion in ausreichend enger physischer Nähe und lang genug stattfindet, damit das Virus übertragen werden könnte – jedoch Individuen betrifft, die einander nicht ausreichend bekannt sind, um sich gegenseitig über ihren Infektionsstatus ohne den Einsatz eines digitalen Tracking-Systems zu informieren.

Realistische Szenarien sind z.B. Begegnungen mit Mitreisenden in einem Zug oder Bus oder längere Interaktionen in Geschäften, Restaurants und ähnlichem. Im Gegensatz dazu scheint das Erfassen von kurzzeitig vorbeigehenden Fremden auf der Straße (da die Interaktion in der

Regel nicht intensiv genug ist) oder das Tracking von Kollegen oder Familienmitgliedern (da sie der infizierten Person ohnehin bekannt sind) von begrenztem Nutzen zu sein.

Dieses Paper befasst sich nicht mit der Verwendung personenbezogener Daten für statistische Zwecke oder politische Beurteilungen (wie z.B. Mobiltelefondaten, die für Bewegungsstatistiken analysiert werden) oder der Verwendung personenbezogener Daten für die Überwachung von Personen in Quarantäne.

2. BEKANNTE TECHNISCHE ANSÄTZE

Derzeit werden zwei Ansätze diskutiert, um mögliche Infektionen mit SARS-CoV-2 zu tracken. Möglicherweise bestehen andere Ansätze, die (noch) nicht in diesem Paper behandelt werden.

2.1. Nachverfolgung über mobile Netzwerkdaten

Verschiedene Medienberichte und politische Debatten haben sich auf die Nutzung von Daten von Mobilfunkbetreibern zur Bekämpfung von SARS-CoV-2 konzentriert. Nach Wissensstand von *noyb*, ist die Standortbestimmung auf der Basis von Mobilfunknetzen nicht exakt genug (Genauigkeit von nur 50 Metern oder mehr), um in den meisten realistischen Szenarien relevante Informationen über die Interaktion zwischen zwei Personen zu erhalten.

> *Beispiel: Wenn sich zwei Mobiltelefon-Benutzer im selben Zug oder im selben Gebäude befinden, ist es unwahrscheinlich, dass die Netzwerkdaten ausreichend genau sind, um zwischen den Waggons oder Räumen des Gebäudes zu unterscheiden.*

Beim derzeitigen Stand der Technik wird eine personalisierte Verfolgung möglicher exponierter Personen auf der Grundlage von Netzwerkdaten technisch kaum durchführbar sein, insbesondere innerhalb von Gebäuden. Angesichts der mangelnden Genauigkeit ist es sehr wahrscheinlich, dass ein solcher Ansatz zu vielen Meldungen und einer „Informationsüberlastung“ führen würde.

2.2. Lokal installierte Tracking-Anwendungen

Der andere Ansatz basiert auf lokal installierten Smartphone-Anwendungen. Diese Anwendungen können auf präzisere Positionsdaten zugreifen, die Kommunikation zwischen den Telefonen ermöglichen und damit die Interaktionen zwischen den Menschen protokollieren.

Es gibt verschiedene technologische Ansätze zur Erzeugung und zum Austausch der notwendigen Interaktionsinformationen (wie Ultraschall, Bluetooth, WiFi, NFC-Signale und/oder GPS-Tracking). Einige dieser Technologien funktionieren sogar in Gebäuden oder Tunneln.

Die weitere Verwendung der generierten Interaktionsinformationen kann in vielen Formen erfolgen, einschließlich der lokalen Speicherung und der Speicherung in einer Cloud, sowie verschiedenen Löschroutinen, Verschlüsselungs- und Pseudonymisierungsansätzen folgen.

Dieses Paper konzentriert sich auf diesen zweitgenannten Ansatz (Tracking basierend auf einer Smartphone- Anwendung), der derzeit realistischster zu sein scheint.

3. VERWENDUNG DER GENERIERTEN TRACKING-DATEN

Der Eingriff in die Grundrechte des Einzelnen hängt von den Folgen der Verarbeitung personenbezogener Daten ab. Bisher scheinen die folgenden Ansätze in Betracht gezogen zu werden:

3.1. Verschiedene Schritte und Verarbeitungsvorgänge

Die meisten Konzepte sehen verschiedene Schritte und Verarbeitungsvorgänge vor für (A) das fortlaufende Tracking personenbezogener Daten („Erfassungsphase“) und (B) die Verwendung von Daten im Falle einer notwendigen Warnung über die Interaktion mit einer SARS-CoV-2-positiven Person („Vorfall“). Für diese unterschiedlichen Situationen und Verarbeitungszwecke können unterschiedliche rechtliche Analysen notwendig sein. Diese Verarbeitungsvorgänge können sogar von verschiedenen für die Verarbeitung Verantwortlichen durchgeführt werden (siehe unten).

Zusätzliche Funktionen (wie „Datenspenden“ zur Bekämpfung von SARS-CoV-2, Funktionen zur Selbsteinschätzung einer möglichen Infektion und andere Informationen) können als separate Verarbeitungsvorgänge angesehen werden, die nicht im Fokus dieses Papers stehen.

3.2. Konsequenzen von Vorfällen

Die Akzeptanz und mögliche Verhaltensänderungen der Benutzer (wie z.B. das Vermeiden von Tests, um die Folgen eines positiven Ergebnisses zu vermeiden) hängen weitgehend von den rechtlichen und praktischen Konsequenzen der Nutzung einer solchen Anwendung ab:

- **Information von Personen**

Einige Ansätze konzentrieren sich auf den Versuch, Personen, die mit einer- SARS-CoV2-positiven Person interagiert haben, pro-aktiv zu informieren, damit diese Personen entsprechend handeln können (wie z.B. einen Test beantragen, sich in Selbstquarantäne begeben, usw.). Dabei wird jedem Individuum die Freiheit gelassen, selbstbestimmte Maßnahmen zu ergreifen – oder die bereitgestellten Informationen sogar zu ignorieren.

- **Identifizierung, Test und Isolierung von positiven Fällen**

Andere Ansätze konzentrierten sich auf den Versuch, Personen, die mit einer SARS-CoV-2-positiven Person interagiert haben, so schnell wie möglich zu identifizieren, zu testen und unter Quarantäne zu stellen.

Dies ist offensichtlich ein viel schwerwiegenderer Eingriff in die Freiheiten des Einzelnen und droht mit einer Vielzahl von Grundrechten (wie Bewegungsfreiheit, Freiheit der Geschäftstätigkeit und Freiheit der Privatsphäre und des Familienlebens) zu kollidieren, die mit der Verarbeitung personenbezogener Daten im Zusammenhang stehen. Der Eingriff ist jedoch auf bestimmte Personen beschränkt. In solchen Fällen kann das öffentliche Interesse

die Rechte des Einzelnen überwiegen. Dies ist hinsichtlich der bestehenden Gesetze, die eine obligatorische Quarantäne vorsehen, anzunehmen.

In der Praxis könnten einige Benutzer abgeschreckt werden, wenn die Verwendung einer Tracking- Anwendung die Einschränkung ihrer Freiheiten zufolge hat.

- **Beschränkung der Bewegungsfreiheit**

Einigen (nicht überprüften) Berichten zufolge schienen einige Länder den umgekehrten Weg zu gehen und die Bewegungsfreiheit *nur* Personen zu gewähren, die eine Anwendung nutzen.

Eine Variante dieses Ansatzes könnte darin bestehen, dass die Nutzung einer Anwendung zu einer *de facto* notwendigen Voraussetzung für die Teilnahme am öffentlichen Leben wird, beispielsweise wenn Unternehmen von ihren Kunden verlangen würden, dass sie eine Tracking-Anwendung verwenden, um ihre Dienste weiterhin nutzen zu können.

Dies folgt dem Ansatz *„infiziert, wenn nicht erwiesenermaßen gesund“* und führt zu einem sehr schwerwiegenden Eingriff in ein breiteres Spektrum von Grundrechten. Gleichzeitig ist dies der Ansatz, den viele europäische Regierungen *de facto* gewählt haben, indem sie eine nationale Ausgangssperre/Bewegungsbeschränkungen für alle Einwohner eines Landes oder eines Gebiets ohne weitere Differenzierung zwischen den einzelnen Personen verordnen. Verschiedene Formen des Trackings von Interaktionen könnten als der verhältnismäßigerer Eingriff in die Grundrechte angesehen werden.

Ausnahmen für Personen, die (vorübergehend) nicht in der Lage sind, bestimmte Formen des Trackings zu nutzen (siehe unten bei 6.5), wären notwendig, um rechtswidrige Diskriminierung und willkürliche Behandlung zu vermeiden.

4. RECHTLICHE ANALYSE GEMÄSS DSGVO

4.1. Verantwortliche

Tracking-Systeme können auf einer zentralisierten Architektur basieren, bei der eine staatliche Stelle oder ein privates Unternehmen (z.B. ein Gesundheitsdienstleister) als „Verantwortlicher“ fungiert.

Alternativ dazu kann ein System auf einem Netzwerk von Endnutzern („Peer-to-Peer“) basieren, wobei jeder Nutzer (je nach Ausgestaltung des Systems) als „Verantwortlicher“ für eine lokale Verarbeitung, wie z.B. ein automatisiertes „Kontaktbuch“, qualifiziert werden kann.

Eine solche Verarbeitung könnte (in begrenzten Situationen und bei strikter technischer Umsetzung) sogar unter die „Haushaltsausnahme“ fallen, die das „Führen von Anschriftverzeichnissen“ (Erwägungsgrund 18 DSGVO) umfasst. Ein lokales „Interaktionsprotokoll“ oder „Kontaktbuch“ könnte (in bestimmten Fällen) als „persönliche oder familiäre Tätigkeit“ interpretiert werden. In solchen begrenzten Situationen würde die lokale Verarbeitung solcher Daten nicht unter die Regelungen der DSGVO fallen.

Eine Kombination verschiedener (gemeinsam) für verschiedene Teile der Verarbeitungsvorgänge Verantwortlicher kann Teil eines Gesamtsystems sein (z.B. wenn ein Gesamtsystem aus einem zentralen Warnsystem und einer lokalen Verfolgung von Interaktionen besteht).

4.2. Personenbezogene Daten

Da das Ziel einer solchen Verarbeitungstätigkeit das Tracking und/oder die Information einer bestimmten infizierten Person oder die Information von Personen ist, die persönliche Begegnungen mit einer infizierten Person hatten, stellen die notwendigen Daten über Interaktionen, Orte und ähnliches in der Regel personenbezogene Daten dar. Per Definition können Daten, die die Identifizierung oder Aussonderung eines App-Benutzers durch den jeweiligen Verantwortlichen und/oder andere App-Benutzer ermöglichen, nicht als anonym bezeichnet werden und müssen als personenbezogene Daten angesehen werden (Artikel 4(1) DSGVO). Hinsichtlich der Verarbeitung solcher personenbezogener Daten gelangt die DSGVO vollumfänglich zur Anwendung.

4.2.1. Besondere Datenkategorien

In den meisten Fällen zielen die Verarbeitungstätigkeiten darauf ab, spezifische Informationen über die Infektion mit SARS-CoV-2 zu übermitteln, die eindeutig Daten über den Gesundheitszustand einer Person darstellen.

In diesem Paper wird daher angenommen, dass die meisten verarbeiteten Daten als „besondere Kategorie“ gemäß Artikel 9(1) DSGVO behandelt werden müssen.

4.2.2. Pseudonymisierte Daten

Bestimmte Elemente eines Tracking-Systems können (und sollten den Grundsätzen von „Datenschutz durch Technikgestaltung" entsprechend) auf pseudonymen Daten basieren (wie Hashes, zufällige IDs und Ähnliches). Solche Daten unterfallen weiterhin der DSGVO und allen relevanten Schutzmaßnahmen, können aber aus Sicht der Datensicherheit erforderlich sein (Artikel 32 DSGVO). Die Verwendung gut gewählter Pseudonyme führt in der Regel zu einem geringeren Potenzial für Missbrauch und Eingriffe in das Recht auf Datenschutz.

4.2.3. Verschlüsselte Daten

Andere Elemente jedes Tracking-Systems können (und sollten den Grundsätzen von „Datenschutz durch Technikgestaltung" entsprechend) auf verschlüsselten Daten basieren.

Solche Daten unterfallen nach wie vor der DSGVO, auch wenn die Daten für bestimmte Informationsinhaber nicht identifizierbar sind (z.B. wenn Tracking-Daten über andere Personen lokal in einem verschlüsselten Format gespeichert werden, wobei eine dritte Partei den Key zur Entschlüsselung hat).

Eine ordnungsgemäße und intelligente Verschlüsselung ist gleichzeitig ein entscheidendes Element, um die Anforderungen der DSGVO, wie Datenminimierung (siehe unten) und Datensicherheit (Artikel 32), zu erfüllen.

4.3. Rechtmäßigkeit der Verarbeitung

Jede Datenverarbeitung muss eine rechtliche Grundlage im Rahmen der DSGVO haben. Ein für die Verarbeitung Verantwortlicher muss eine oder mehrere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten wählen. Es kann verschiedene Rechtsgrundlagen für verschiedene Verarbeitungsvorgänge geben. In der DSGVO finden sich mehrere Rechtsgrundlagen, auf deren Basis die Verarbeitung von Daten zum Tracking von SARS-CoV-2-Infektionen erfolgen kann.

4.3.1. Einwilligung

Wie bei jeder Verarbeitung kann die betroffene Person in die Verarbeitung von personenbezogenen Daten einwilligen. Angesichts der Sensibilität der Daten und des schwerwiegenden Eingriffs in das Recht auf Datenschutz kann dies bei den meisten Verarbeitungsvorgängen der bevorzugte Ansatz sein.

Besondere Aufmerksamkeit muss darauf gerichtet werden, dass die Einwilligung „freiwillig", „für den bestimmten Fall", „ausdrücklich" (oder „eindeutig") und „in informierter Weise" erteilt wird. Im Zusammenhang mit Beschäftigungsverhältnissen oder bei staatlichen Maßnahmen kann die Einwilligung in der Regel nicht als freiwillig erteilt angesehen werden.

Die Einwilligung sollte idealerweise bei der Installation einer Anwendung oder bei jeder Interaktion mit einem anderen Benutzer abgegeben werden. Die Anwendung kann es ermöglichen, die Bedingungen zu definieren, unter denen ein Benutzer der Nutzung der Daten zustimmt (wie z.B. nur zum Zweck des gegenseitigen Trackings zur Bekämpfung von SARS-CoV-2, begrenzt auf eine bestimmte Dauer und ähnliches).

In den meisten realistischen Szenarien scheint es, dass das Tracking von Interaktionen mit anderen Personen in der Erfassungsphase sowie jede Benachrichtigung im Falle eines „Vorfalls“ auf der Einwilligung der Person basieren kann, die die Anwendung installiert hat.

Das Tracking anderer Benutzer, die keine Anwendung installiert haben (z.B. wenn ein System nicht zwischen den IDs von Smartphones, die die Anwendung installiert haben, und denen, die sie nicht installiert haben, unterscheiden kann), müsste auf einer anderen rechtlichen Grundlage beruhen.

4.3.2. Lebenswichtige Interessen

In Erwägungsgrund 46 DSGVO wird die „*Überwachung von Epidemien und deren Ausbreitung*“ ausdrücklich als „lebenswichtiges Interesse“ der betroffenen Person oder eines Dritten erwähnt. Es kann daher davon ausgegangen werden, dass die Verarbeitung von Daten für solche Zwecke der Wahrung „lebenswichtiger Interessen“ der betroffenen Person oder eines Dritten dient.

Artikel 6(1)(d) DSGVO („lebenswichtige Interessen“) gilt nicht für besondere Datenkategorien. Folglich erlaubt diese Rechtsvorschrift nur die Verarbeitung von Daten, die keine besondere Kategorie nach Artikel 9 DSGVO darstellen.

> *Beispiel: Die Erfassung von Kontaktdaten in einer „Kontaktliste“ (z.B. Bluetooth-Kennungen während der „Erfassungsphase“) gibt in der Regel keine besondere Datenkategorie (wie Gesundheitsinformationen) preis, ist aber notwendig, um eine Person im Falle eines „Vorfalls“ zu benachrichtigen. Die Erfassung solcher Informationen kann sich möglicherweise auf Artikel 6(1(d) DSGVO stützen.*

Da Artikel 9(2)(c) DSGVO verlangt, dass besondere Datenkategorien nur dann für ein „lebenswichtiges Interesse“ verwendet werden dürfen, wenn die betroffene Person zusätzlich zu den Anforderungen in Artikel 6(1)(d) DSGVO „*aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben*“, erscheint es unwahrscheinlich, dass dies eine geeignete Rechtsgrundlage für die Verarbeitung besonderer Datenkategorien sein könnte, sobald ein Vorfall eintritt.

> *Beispiel: Die Einwilligung oder eine andere gesetzliche Grundlage gemäß Artikel 9(2) DSGVO scheint für die Benachrichtigung anderer Nutzer über einen „Vorfall“ notwendig zu sein, da es sich dabei um Daten über die Gesundheit der infizierten und der potenziell exponierten Person handelt.*

Wann immer die Verarbeitung zur Bekämpfung von SARS-CoV-2 ein „lebenswichtiges Interesse“ darstellt, sollte sich die Frage nicht stellen, ob die Verarbeitung auch auf ein „berechtigtes Interesse“ gemäß Artikel 6(1)(f) DSGVO gestützt werden kann. Andernfalls wäre die übliche Interessenabwägung gemäß Artikel 6(1)(f) DSGVO vorzunehmen.

4.3.3. Unionsrecht oder der Recht eines Mitgliedstaats

Artikel 9(2)(i) DSGVO sieht vor, dass das Recht der Union oder eines Mitgliedstaates die Verarbeitung im Falle „*schwerwiegender grenzüberschreitender Gesundheitsgefahren*“ zulassen oder vorschreiben kann. SARS-CoV-2 erfüllt diese Definition eindeutig. Die

Bestimmung verlangt gleichzeitig „a*ngemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person*“.

Während Artikel 9(2)(i) DSGVO für die meisten Verarbeitungsvorgänge während der SARS-CoV-2-Krise die *lex specialis zu* sein scheint, erlaubt Artikel 9(2)(g), (h) und (j) DSGVO den Mitgliedstaaten auch, nationale Gesetze zu erlassen, die die Verarbeitung besonderer Kategorien personenbezogener Daten aus Gründen eines erheblichen öffentlichen Interesses, bestimmter medizinischer und gesundheitlicher Versorgungszwecke oder für Forschungs- und Statistikzwecke vorsehen. Jedes derartige nationale Gesetz muss spezifische und geeignete Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen vorsehen. Dies bedeutet im Wesentlichen, dass solche nationalen gesetzlichen Maßnahmen nur dann mit dem Grundrecht auf Privatsphäre und Datenschutz in Konflikt geraten dürfen, wenn dies zur Erreichung des Ziels geeignet, notwendig und angemessen ist.

Es kann bestehende nationale Gesetze (z.B. Gesetze über Infektionskrankheiten) oder neu geschaffene gesetzliche Maßnahmen zur Bekämpfung von SARS-CoV-2 geben. In diesem Paper wird nicht bewertet, ob eine bestimmte bestehende oder vorgeschlagene nationale Regelung in den Mitgliedstaaten der DSGVO entspricht.

- **Rechtliche Grundlage für die Verarbeitung personenbezogener Daten („Erlaubnis“)**

Ein Gesetz kann bestimmte Datenverarbeitungen *zulassen*, wobei es dem für die Verarbeitung Verantwortlichen überlassen bleibt, ob er persönliche Daten verarbeiten will (wie eine allgemeine Erlaubnis zur Verwendung personenbezogener Daten für das Tracking).

- **Pflicht zur Verarbeitung und/oder Bereitstellung personenbezogener Daten („Pflicht“)**

In vielen Fällen werden Gesetze bestimmte Verarbeitungen personenbezogener Daten (wie z.B. Meldepflichten für Infektionskrankheiten) *vorschreiben*. Dies kann die Gestaltung eines Tracking-Systems beeinflussen.

> *Beispiel: Ein System kann so konzipiert sein, dass es entweder eine „Melde“-Funktion enthält oder im Gegenteil so konzipiert ist, dass die Informationspflichten für den einzelnen Benutzer nicht gelten, weil die Daten so verschlüsselt oder pseudonymisiert sind, dass ein Benutzer unmöglich einer Meldepflicht für eine infizierte Person unterliegen kann.*

Eine vertiefte Analyse spezifischer Gesetze würde den Rahmen dieses Papers sprengen, scheint aber entscheidend zu sein, um unbeabsichtigte Konsequenzen oder überraschende rechtliche Pflichten der Nutzer einer Anwendung zu vermeiden.

4.4. Zweckbindung

Das Prinzip der Zweckbindung ist das „Rückgrat“ jeder Datenschutzanalyse. Die meisten anderen Elemente der DSGVO-Analyse beziehen sich auf den gewählten spezifischen Zweck.

Die Zwecke müssen spezifisch genug sein, um ein gutes Verständnis der Datennutzung zu ermöglichen. So ist z.B. die „Prävention weiterer SARS-CoV-2-Infektionen“ nicht spezifisch genug. Beispiele für relevante Zwecke können sein:

- Bereithaltung der Interaktionsinformationen für das Tracking von SARS-CoV-2,

- die Information von Personen über eine SARS-CoV-2-Exposition,
- die Information der Gesundheitsbehörden über SARS-CoV-2-Expositionen oder
- Bestätigung (z.B. gegenüber einem Dritten), dass es keine bekannten Expositionen des Benutzers gibt.

Der tatsächliche und genaue Zweck hängt von den Funktionalitäten der Anwendung oder des Tracking-Systems ab. Für jede Funktion einer Anwendung kann es zahlreiche Verwendungszwecke geben.

4.4.1. Weiterverarbeitung

Unter bestimmten Bedingungen kann die DSGVO die sekundäre Verwendung von personenbezogenen Daten für andere, ursprünglich nicht vorgesehene Zwecke zulassen (z.B. nach Artikel 6(4) DSGVO).

Es ist jedoch notwendig, dass vorhersehbare Zwecke (wie Forschung und Statistik) in die ursprüngliche Liste der Zwecke aufgenommen werden (Artikel 13(1)(c) DSGVO). Die Verarbeitung von Daten für solche Zwecke muss in der Regel fakultativ sein und auf der Einwilligung des Nutzers beruhen. Beruht sie auf anderen Rechtsgrundlagen, so ist der Nutzer ordnungsgemäß zu informieren und – bei einer Verarbeitung aufgrund eines berechtigten Interesses – muss die Möglichkeit eines „Opt-out“ bestehen.

Im Allgemeinen ist es möglich, den Benutzern zu erlauben, ihre personenbezogener Daten für nützliche, aber nicht notwendige Verarbeitungen zu „spenden“. Angesichts des Kampfes gegen SARS-CoV-2 ist es auch sehr wahrscheinlich, dass die Nutzer einer solchen Zweitverwendung zustimmen.

4.5. Datenminimierung

4.5.1. Allgemeines Prinzip

Der allgemeine Grundsatz der Datenminimierung soll sicherstellen, dass nur das für den Zweck erforderliche Minimum an Daten verarbeitet wird. Dies bedeutet nicht, dass die Sammlung von Informationen so weit eingeschränkt werden muss, dass der Zweck nicht mehr erfüllt werden kann. Alle Informationen, die für den Zweck der Verarbeitung notwendig sind, können verarbeitet werden. Liefert ein Verarbeitungsvorgang keine ausreichend genauen Daten als Ergebnis, ist es möglicherweise notwendig, weitere relevante Daten zu verarbeiten, um eine ausreichende Genauigkeit zu erreichen.

Beispiele für Daten, die (je nach System) relevant sein können:

- Datum und Uhrzeit einer Interaktion
- Ort einer Interaktion
- Dauer einer Interaktion
- Kennung der Person, mit der der Benutzer interagiert hat

Beispiele für Daten, die (je nach System) möglicherweise nicht relevant sind:

- Daten über Personen, die nicht an einem Tracking-System teilnehmen

- Gerätekennungen oder Verfolgungsinformationen, die aus medizinischer Sicht nicht relevant sind
- Exakte Zeitstempel, Orte und Ähnliches, wenn weniger spezifische Informationen (z.B. nur das Datum statt des exakten Zeitstempels) ausreichen.

4.5.2. Systemdesign nach „need to know"-Basis

Jedes Tracking-System benötigt mehrere Akteure (idealerweise die Mehrheit der Bevölkerung), um personenbezogener Daten gemeinsam zu teilen und zu verarbeiten. Nur eine größtmögliche Begrenzung der verfügbaren Daten für jeden einzelnen Akteur kann zu einem Gesamtsystem führen, das die Grundrechte auf Datenschutz und Privatsphäre ausreichend berücksichtigt. Dies lässt sich durch einen strikten „need to know"-Ansatz umsetzen, bei dem der Zugang zu den Daten streng auf jene Personen und Einrichtungen beschränkt ist, die die Daten verarbeiten müssen, wobei angemessene technische Maßnahmen zur Umsetzung eines solchen Ansatzes vorgesehen werden müssen.

4.5.2.1. Daten, die einem zentralen Administrator zur Verfügung stehen

Es kann bestimmte Daten („Account-Informationen") geben, die ein zentraler Administrator möglicherweise benötigt, um die Identität des einzelnen App-Benutzers zu überprüfen. Verantwortliche, die als zentrale Administratoren fungieren, können versuchen, den Umfang solcher Daten einzuschränken oder nur in bestimmten Situationen weitere Informationen über die Identität des Benutzers zu verlangen (z.B. wenn ein Benutzer einen Vorfall meldet oder medizinische Hilfe benötigt).

Andere Informationen, wie z.B. die Verwendung von Statistiken, sollten auf anonymen Daten basieren.

4.5.2.2. Daten, die einem normalen Benutzer zur Verfügung stehen („Erfassungsvorgang")

Der App-Benutzer, der keine Aufgabe als zentraler Administrator hat, scheint während des Erfassungsvorgangs eines Tracking-Systems keinen Zugriff auf persönliche Informationen anderer Personen zu benötigen. Je nach Wahl des Designs und der Privatsphäre-Einstellungen können solche Daten lokal oder in einem zentralisierten System gespeichert werden.

Die Identifizierungsdaten, die vom Gerät der Personen, mit denen der App-Benutzer in Kontakt war, bereitgestellt werden, können pseudonymisiert oder verschlüsselt werden. Dies kann erfolgen bevor oder nachdem sie dem App-Benutzer mitgeteilt werden und soll sicherstellen , dass ein Benutzer nicht auf die personenbezogenen Daten anderer Benutzer zugreifen kann.

Die lokale Kontaktliste kann dadurch vollständig von dem Benutzer, der die Informationen sammelt, abgeschirmt werden. Daten, die für den Benutzer nicht oder nicht mehr erforderlich sind, sollten automatisch gelöscht werden, z.B. wenn die potenzielle Inkubationszeit des Virus abgelaufen ist.

4.5.2.3. Daten, die der infizierten Person zur Verfügung stehen („Vorfall“)

Wenn eine Person bekanntermaßen infiziert ist („Vorfall“), sollte diese Person im Idealfall nicht mehr tun müssen, als diese Tatsache in einer verifizierbaren Weise zu melden. Um Falschmeldungen zu vermeiden, könnte eine Form der Zulassung/Überprüfung sichergestellt werden (z.B. eine Bestätigung durch medizinisches Fachpersonal, das den SARS-CoV-2-Test durchgeführt hat).

Die infizierte Person braucht nicht zu wissen, welche exponierten Personen informiert werden.

Eine vertrauenswürdige Drittpartei (z.B. ein Gesundheitsdienstleister oder eine behördliche Einrichtung) könnte sich um die Entschlüsselung, Überprüfung und Analyse der gesammelten Daten kümmern und die Benachrichtigung exponierter Dritter auslösen.

4.5.2.4. Daten, die der exponierten Person zur Verfügung stehen („Vorfall“)

Wenn eine Person eine Infektion meldet, darf die exponierte Person nur über die Tatsache informiert werden, dass sie exponiert war. Solche Informationen können über einen zentralisierten Kommunikationsdienst oder über ein „Peer-to-Peer“-System übermittelt werden.

Zusätzliche Informationen können relevant sein, um zu verstehen, wie schwerwiegend die Exposition war oder wie lange realistischerweise mit einem Ausbruch von Symptomen gerechnet werden kann. Solche zusätzlichen Informationen können jedoch das Recht auf Privatsphäre der infizierten Person beeinträchtigen, da sie die Identität der infizierten Person preisgeben können.

Um diese widersprüchlichen Interessen auszugleichen, kann es nötig sein, solche Informationen in einem Format bereitzustellen, das abstrakt genug ist (z.B. nur der Tag der Infektion und die ungefähre Dauer der Exposition oder ein „Expositionscore“), um die relevanten Informationen zu liefern, gleichzeitig aber auch die Anonymität der infizierten Person so weit wie möglich zu gewährleisten.

4.5.2.5. Daten, die den Behörden / Gesundheitsdienstleistern zur Verfügung stehen

Je nach nationaler Gesetzgebung oder der Gestaltung des Systems müssen die Daten möglicherweise an Behörden oder Gesundheitsdienstleister weitergegeben werden. Das System kann absichtlich vorsehen keine solchen meldepflichtigen Informationen zu verarbeiten, um derartige Informationspflichten zu umgehen (z.B. um das Vertrauen der Nutzer in die Anonymität des Systems zu stärken).

4.6. Richtigkeit der Daten

Gerade bei einem so sensiblen Thema wie der Infektion mit einem hoch ansteckenden Virus oder der Exposition gegenüber einem Virus ist die Genauigkeit und Qualität der Daten von größter Bedeutung.

Es wäre kontraproduktiv und würde sogar den Zweck der Verarbeitungstätigkeit vereiteln, wenn die Nutzer entweder falsche oder zu viele (irrelevante) Meldungen über eine mögliche Exposition („Informationsüberlastung“) oder zu wenige oder verspätete Meldungen erhalten. Einige Beispiele, die in Betracht gezogen werden können, um sicherzustellen, dass korrekte Daten zur Verfügung gestellt werden:

- *Besonderes Augenmerk muss auf eine genaue technische Analyse der Interaktion zwischen zwei Personen und jede möglichen Logik oder jeden Algorithmus gelegt werden, der entscheidet, welche exponierten Personen informiert werden müssen. Eine Entscheidung darüber, welche Person informiert werden muss, könnte z.B. auf die Nähe, den Zeitrahmen (Zeitpunkte, zu denen ein Patient wahrscheinlich mehr oder weniger infektiös war), die Dauer der Interaktionen oder die Frage gestützt sein, ob die Begegnung innerhalb eines Gebäudes, während des Transports oder im Freien stattfand (z.B. auf der Grundlage von GPS-Standorten). Eine solche Analyse der Rohdaten darf nur im Falle eines bestätigten „Vorfalls“, bereits während der Erfassungsphase oder einer Kombination davon, erfolgen.*
- *Ebenso muss ein System der exponierten Person ausreichend genaue Informationen zur Verfügung stellen, damit sie die entsprechenden Schritte einleiten kann. Die Optionen können von einer rein binären Information, einem „Expositionsscore“ oder bis zu kontextbezogenen Informationen wie Tag, Dauer, Ort und räumlicher Nähe reichen.*
- *Schließlich scheint es wichtig, dass die Benutzer nicht im Alleingang ungenaue Informationen (wie die Selbstberichterstattung als positiv/negativ ohne eine unabhängige Überprüfung) liefern können.*

Während die Richtigkeit der Informationen aus medizinischer Sicht gemeinsam mit medizinischen Experten beurteilt werden muss, ergibt sich auch aus Artikel 5 DSGVO eine Pflicht zur Bereitstellung genauer Informationen.

4.7. Speicherbegrenzung

Das Prinzip der Speicherbegrenzung verlangt, dass personenbezogene Daten nicht länger als nötig aufbewahrt werden. Die Fristen müssen sich an der medizinischen Relevanz (wie z.B. Infektionszeiten) sowie an realistischen Zeiträumen für eventuell erforderliche administrative Schritte orientieren.

> *Beispiel: Die Daten können für realistische Infektionszeiten und realistische SARS-CoV-2-Testzeiten aufbewahrt werden, um sicherzustellen, dass die Daten nicht gelöscht werden, bevor ein positives Testergebnis vorliegt, dürfen aber auch nicht länger als unbedingt notwendig aufbewahrt werden.*

Es ist zwingend erforderlich, dass die Daten gelöscht werden, sobald sie zur Erfüllung der entsprechenden Zwecke nicht mehr geeignet sind.

4.8. Sicherheit der Daten

Ein Tracking-System wäre ein Hauptziel für viele Akteure, und sei es nur, um zu testen, ob die Sicherheit der Systemarchitektur gewährleistet ist. Angreifer können ihre eigenen Anwendungen entwickeln, die mit einem System oder anderen Anwendungen interagieren, aber falsche Daten liefern oder Daten für illegale Zwecke sammeln. Angesichts der Sensibilität der verarbeiteten Daten, aber auch der Notwendigkeit des öffentlichen Vertrauens in ein

SARS-CoV-2-Tracking-System muss die Datensicherheit im Mittelpunkt eines jeden vorgeschlagenen Systems stehen und gleichzeitig „angemessen“ (Artikel 32 DSGVO) sein, im Hinblick auf diese Risiken und die Folgen des Missbrauchs.

5. DATENSCHUTZ DURCH TECHNIKGESTALTUNG

Jedes Tracking-System, das eine breite gesellschaftliche Akzeptanz finden soll, muss unter Berücksichtigung des Datenschutzes konzipiert sein. Dies sollte über den Wortlaut der DSGVO in Artikel 25 DSGVO hinausgehen und den Anspruch haben auf einer möglichst datenschutzfreundlichen Architektur zu basieren.

5.1. Lokale Speicherung

Viele technische Lösungen beruhen auf der lokalen Speicherung von Interaktionsinformationen („Self-Tracking“).

Dies kann dem einzelnen Nutzer faktische Macht über die Daten geben, da die Daten physisch in der Hand des Nutzers bleiben. Es sollte sichergestellt werden, dass die Daten auf sichere Weise gespeichert werden und weder für das Betriebssystem noch für andere Anwendungen auf dem Telefon des Nutzers zugänglich sind.

Lokale Speicherung bedeutet auch, dass die Daten anderer getrackter Personen vom Gerätebesitzer eingesehen werden können. Strategien zur Begrenzung des Zugriffs können die Verschlüsselung oder Pseudonymisierung solcher Informationen vor der Übertragung oder Speicherung auf dem lokalen Gerät umfassen.

5.2. Verschlüsselung (öffentliche/private Schlüssel)

Insbesondere in Situationen, in denen potentiell Millionen von Benutzern personenbezogene Daten anderer Menschen verarbeiten, kann eine starke Verschlüsselung sicherstellen, dass die Daten gemeinsam genutzt werden können, während gleichzeitig verhindert wird, dass jeder Empfänger diese Daten missbrauchen und offenlegen kann.

Asymmetrische Kryptographie ist besonders geeignet, dieses Ziel zu erreichen. Der Schlüsselaustausch kann zum Beispiel auf einer Peer-to-Peer-Basis oder über vertrauenswürdige Institution erfolgen.

5.3. „Zwei-Personen-Regel“

Als weitere Vorsichtsmaßnahme kann die Verwendung personenbezogener Daten (insbesondere im Falle einer Infektion) auf der „Zwei-Personen-Regel“ basieren, d.h. zwei Akteure (z.B. die infizierte Person und ein Angehöriger eines Gesundheitsberufs) müssen einen Schlüssel eingeben, um einen Verarbeitungsvorgang wie die Entschlüsselung von Daten oder die Benachrichtigung von exponierten Personen auszulösen.

5.4. Pseudonymisierung

Immer dann, wenn eine anonyme oder verschlüsselte Verarbeitung von Informationen nicht möglich ist, müssen Pseudonyme verwendet werden, um die verarbeiteten personenbezogenen Daten zu verschleiern.

Pseudonymisierte Daten sind nach den einschlägigen Bestimmungen der DSGVO nicht privilegiert und müssen wie normale personenbezogene Daten behandelt werden.

5.5. Unabhängige Verifizierung

Um die Richtigkeit von persönlichen Daten, die über ein System weitergegeben werden, zu gewährleisten, können Formen der unabhängigen Überprüfung eingeführt werden. Ein System muss zum Beispiel sicherstellen, dass Benutzer keine falschen Informationen eingeben und ungenaue Benachrichtigungen auslösen können.

5.6. Dienstleistungen von Dritten

Entwickler nutzen regelmäßig Dienste, Plug-Ins und SDKs von Drittanbietern. Solche Elemente erfordern häufig Datenübertragungen in Drittländer. Dies *kann* zwar mit der DSGVO vereinbar sein, aber die bloße Erwähnung, dass Dritte Zugang zu (einigen) personenbezogenen Daten haben, kann zur Ablehnung durch die Benutzer führen. Typische Beispiele sind Cloud-Hosting durch Dritte, SDKs zur Fehlerverfolgung oder Funktionen des Betriebssystems zur Anzeige von Benachrichtigungen an die Benutzer.

Die Wahl des Designs zwischen Benutzerfreundlichkeit und Datenschutz kann den Präferenzen der Benutzer überlassen werden, wenn sie sich für zusätzliche Funktionen „entscheiden“ können.

5.7. (Im Konflikt stehende) Rechte nach der DSGVO und anderen Gesetzen

Die Nutzer können ihre Rechte als betroffene Personen gegenüber dem jeweiligen für die Verarbeitung Verantwortlichen geltend machen. Dies kann mit den Interessen anderer Nutzer in Konflikt geraten (z.B. wenn eine infizierte Person wissen will, wer die Empfänger der Benachrichtigung sind, siehe Artikel 15(1) DSGVO).

Benutzer können auch von der (ordnungsgemäßen) Nutzung bestimmter Anwendungen oder Systeme Abstand nehmen, wenn nationale Gesetze den für die Verarbeitung Verantwortlichen verpflichten, Daten an staatliche Stellen zu übermitteln.

Eine strikte „Need to know“-Basis kann es dem Verantwortlichen ermöglichen, solche Anfragen unter Berufung auf nationale Gesetze und/oder Artikel 11(2) DSGVO zu bearbeiten.

6. SONSTIGE EINSTELLUNGEN

Obwohl nicht direkt mit einer rechtlichen Analyse im Rahmen der DSGVO verbunden, erscheinen die folgenden Punkte in einem *Ad-hoc*-Paper über SARS-CoV-2-Tracking-Systeme erwähnenswert:

6.1. Ausreichende Akzeptanz

Jedes SARS-CoV-2-Tracking-System hängt stark von der Akzeptanz eines großen Teils der Gesellschaft ab. Eine gute Datenschutzpraxis ist sicherlich eine Voraussetzung für eine breite Akzeptanz eines Tracking-Systems in der Öffentlichkeit.

6.2. Interoperabilität

Insbesondere (konkurrierende) private Initiativen können bei der Entwicklung eines SARS-CoV-2-Tracking-Systems eine gewisse Interoperabilität mit anderen Anwendungen oder Systemen in Betracht ziehen. Dies kann auch bestimmte zusätzliche Verarbeitungsaktivitäten erfordern, z.B. für den Datenaustausch zwischen Anwendungen oder zwischen Geräten. Die Interoperabilität kann folglich auch unterschiedliche Rechtsgrundlagen für die Verarbeitung nach Artikel 6 und 9 DSGVO erfordern. Darüber hinaus müssen bei der Entwicklung interoperabler technischer Lösungen die Grundsätze des „Datenschutzes durch Technikgestaltung“ beachtet werden.

6.3. Sozialer Druck

Sozialer Druck für ist jeden, der ein SARS-CoV-2-Tracking-System initiiert, wünschenswert, da dies ein Schlüsselfaktor für die Nutzung eines jeden Systems sein kann. Jedoch ist eine freiwillig abgegebene Einwilligung betreffend ein Tracking-System unter Umständen nicht möglich, wenn es *de facto* unmöglich ist, die Nutzung zu verweigern (z.B. wenn private Einrichtungen die Bereitstellung von Dienstleistungen von der Nutzung einer Anwendung abhängig machen). Dasselbe gilt im Beschäftigungskontext, in dem die Einwilligung eines Mitarbeiters als nicht freiwillig abgegeben gilt.

6.4. Verhaltensänderungen

Abhängig vom rechtlichen und technischen Zusammenspiel können Überwachungs- und Tracking-Maßnahmen auch zu einem Verhalten führen, das die Tracking-Bemühungen untergräbt.

> *Beispiel: Wenn ein SARS-CoV-2-Test zu Quarantänemaßnahmen, zu einer zu breiten Information Dritter über den Gesundheitszustand, zu Diskriminierung und ähnlichem führt, versuchen manche Menschen möglicherweise, einen Test zu vermeiden. Wenn die Informationen durch eine Anwendung zu der Pflicht führen, getestet zu werden, können Menschen die Nutzung der Anwendung vermeiden.*

Solche Verhaltensänderungen und mögliche Ausweichmanöver müssen im Anwendungsdesign berücksichtigt werden.

6.5. Begrenzter Zugang zu Technologie

Es kann nicht davon ausgegangen werden, dass jeder Mensch Zugang zu einem modernen Smartphone hat, das voll funktionsfähig und aufgeladen ist. Auch überschreiten Mobiltelefonnutzer regelmäßig ihr Downloadvolumen.

Andere verwenden möglicherweise alternative Betriebssysteme (wie Blackberry oder „offene“ Android-Derivate) oder traditionelle Mobiltelefone. Einige Benutzer verwenden möglicherweise keine Google- oder Apple-Accounts, die zum Herunterladen von Anwendungen von ihren jeweiligen App-Plattformen erforderlich sind.

Kinder haben in der Regel überhaupt keine Mobiltelefone. Besonders ältere (und daher gefährdete) Menschen haben möglicherweise gar kein Mobiltelefon oder benutzen keine Smartphones. Mobiltelefone, die für ältere Menschen konzipiert sind, verwenden möglicherweise kein iOS- oder Android-Betriebssystem und können keine externen Anwendungen ausführen. Viele solcher Telefone sind im Wesentlichen nur „Feature-Telefone“.

6.6. Open Source & unabhängige Verifizierung

Die Implementierung als Open-Source-Software sowie andere Formen der unabhängigen Verifizierung können entscheidende Elemente sein, um eine hohe Qualität und das Vertrauen in jedes Verfolgungssystem zu gewährleisten. Dies kann unabhängig vom Lizenzmodell sein (z.B. wenn der Code veröffentlicht wird, das Urheberrecht jedoch bei einer Instanz verbleibt, um die ordnungsgemäße Nutzung des Codes zu gewährleisten).

Offene Lizenzen können die gemeinsame Nutzung von Technologie durch Länder und Entwickler ermöglichen – insbesondere für weniger entwickelte Regionen oder Länder, die zu klein sind, um ein eigenes Tracking-System zu betreiben.

6.7. „Hinlenken“ als sanfterer Weg, um die Annahme eines Systems sicherzustellen

Verschiedene Formen des „Hinlenkens“ könnten genutzt werden, um die Nutzung einer Anwendung zu fördern (z.B.: ein Guthaben von EUR 10,- durch den Mobilfunkbetreiber für jeden, der die Anwendung installiert hat, Ermutigung durch „Badges“, die in sozialen Netzwerken geteilt werden können und ähnliches).

6.8. Andere Verarbeitungsvorgänge

Anwendungen können zusätzliche relevante Informationen verarbeiten (wie die Information, dass ein Benutzer einen negativ auf SARS-CoV-2 getestet wurde, Informationen über bloße Symptome und ähnliches) und es Benutzern erlauben, zusätzliche Informationen für Forschung, öffentliche Gesundheit und Statistik zu teilen („spenden Sie Ihre Daten“).

Anwendungen sollten sicherstellen, dass solche unterschiedlichen Funktionen unabhängig von der Kernfunktion zum Tracking von Daten nutzbar sind. Zwar ist es durchaus wahrscheinlich, dass eine große Mehrheit der Nutzer sich für eine zusätzliche Verarbeitung zum öffentlichen Wohl „entscheidet“, aber diese Verarbeitung kann andere auch davon abhalten, die Kernfunktionalität der Anwendung zu nutzen. Die DSGVO würde auch keine

„gebündelte“ Einwilligung für Funktionen zulassen, die von notwendigen Verarbeitungen getrennt werden können.

KONTAKT & FEEDBACK

Wir freuen uns sehr darauf, dieses Paper weiter zu verbessern. Sollten Sie Rückmeldungen zu diesem *Ad-hoc*-Paper haben oder weitere Unterstützung bei der Entwicklung eines Systems oder einer Anwendung zur Bekämpfung von SARS-CoV-2 benötigen, zögern Sie nicht, unser Legal-Team unter info@noyb.eu zu kontaktieren.